REMARKS

This application has been reviewed in light of the Office Action dated February 8, 2008. Claims 1-21 are pending in this application, with claims 1, 10, 19 and 20 being in independent form. Claims 1, 3, 10, 12 and 19 have been amended as described in more detail below. Favorable reconsideration is respectfully requested.

The Office Action rejected claims 1-9 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicant regards as the invention. The Examiner stated in the Office Action that it was "unclear how the client hashes the nonce before it receives the nonce." In response to this rejection Applicant has amended claim 1 to more clearly define the invention as recited therein. More specifically, claim 1 has been amended to recite that a hash value of parameters including the nonce value is received from the client computer after the server responds with a nonce value, which finds support in claim 1 as originally filed. With this amendment, the recitations in amended claim 1 better correspond to the wording of pending claim 20. In addition, Applicant submits that it is thus clear that the client computer first receives a nonce numerical value from the server in response to an authentication request (see feature of claim 1 "said server responding with an N byte nonce numerical value"), and then sends a hash value computed using a hash algorithm and parameters including the nonce value.

The Office Action rejected claim 19 under 35 U.S.C. § 101, asserting that the claim is directed to non-statutory subject matter. Applicant has amended claim 19 to be directed to a network for at least one of data and telecommunication, rather than a medium as previously claimed. Applicant therefore submits that the rejection is moot and the subject matter of claim 19 is directed to tangible subject matter.

The Office Action rejected claims 1-21 under 35 U.S.C. § 103(a) as being unpatentable over U.S. published Application No. 2004/0187024 (Briscoe) in view of U.S. published Application No. 2004/0249974 (Alkhatib). Applicant respectfully traverses this rejection for the reasons stated below.

Further to Applicant's response as filed on November 29, 2007, Applicant is still of the opinion that the present invention as defined by the pending claims is non-obvious in view of the cited prior art documents.

First, as a general comment, it is noted that Briscoe et al. teaches an authentication method that consists of two procedures, namely a procedure for distribution of authentication information among the clients of the network (paragraphs [0045]-[0054]), and a procedure for authentication of a network client using the authentication information of at least three other clients within the network (paragraphs [0059]-[0066]). These two procedures are clearly identified and separated (paragraph [0058]). In the Office Action, the Examiner randomly mixes features of the distribution procedure where, for example, messages are identified by means of signatures as cookies and features of the authentication procedure. A person skilled in the art would have major difficulties knowing how to mix the features of these two different procedures since there is no discussion regarding this point in Briscoe et al. In addition, claim 1 is patentable over Briscoe et al. at least because claim 1 includes the following recitation:

"receiving from a client computer an authentication request containing a clients username to a server providing said services, said server identifying said client computer IP address and client password accessible by the server through the transmitted username."

Regarding this feature, the Examiner states that Figure 3 of Briscoe et al. teaches this recitation. However, Figure 3 does not teach or suggest that the computer IP address and password of the client need to be authenticated. Instead, Figure 3 shows an authentication request message including the IP addresses and secret client IDs for each client from which the client being authenticated is to seek authentication information (paragraph [0060]). In the example disclosed by Briscoe et al, the authentication request message comprises information about three other clients of the network (Figure 3 and paragraph [0061]).

Claim 1 is also patentable over Briscoe et al. at least because claim 1 contains the recitation directed to:

"the server responding with an N byte nonce numerical value."

For this feature, the Examiner refers to the "issuing network entity" of Briscoe et al., in particular paragraph [0045]. However, this issuing entity corresponds to the client and not to the server, as discussed in paragraph [0045] by "the cookie ... can only be generated by the particular, issuing network entity, i.e. the client since ...." Furthermore, the issuing network entity of paragraph [0045] does not send any nonce value, only a cookie comprising a hash of the server's IP address B, the client's IP address A and the local secret of the client.

Claim 1 is also patentable over Briscoe et al. at least because claim 1 contains the recitation directed to:

"a hash value of at least the parameters clients password, client computer unique IP address, server unique IP address and the nonce value"

For this feature, the Examiner refers again to paragraph [0045] where it is disclosed that the client creates a cookie comprising a hash of the server's IP address B, the client's IP address A and the local secret of the client. There is therefore no nonce value involved in the hash disclosed in paragraph [0045] of Briscoe et al. In fact, the authentication request of Briscoe et al. comprises information about three other clients of the network (paragraphs [0060]-[0061]), i.e. no information about the client to be authenticated.

Although claim 1 has been amended in response to the Section 112 rejection described above, Applicant notes that the Examiner rejected claim 1 in relation to the recitation directed to "receiving the hash value from the client computer as an authenticator for accessing the services." In making this rejection, the Examiner refers to paragraph [0046] where, indeed, the server receives from the client a message including a cookie with a hash. However, we note for the record that, in the document of Briscoe et al., the communication between the client and the server disclosed in paragraph [0046] corresponds to the verification of messages within the procedure for distribution of authentication information. As such, this verification does not result in access to services at the server.

Claim 1 is also patentable over Briscoe et al. at least because claim 1 contains the recitations directed to:

"said server reproducing said authenticator by utilizing said hash algorithm and the parameters clients accessible password, client computer unique IP address, server unique IP address, and said nonce value, comparing the reproduction with the transmitted authenticator, and granting an access to said server and services if said reproduced authenticator matches said transmitted, thus by utilizing said client computer unique IP address and said server unique IP address in said authenticator preventing a man-in-the-middle computer, having a different IP address, from addressing said server with a matching authenticator."

For these features, the Examiner refers to paragraph [0064] where a response sent by the client within the authentication procedure is verified by the server using two signatures. If the signatures sent by the client are matched with those stored at the server, the server processes the response. Thus, the verification process disclosed in paragraph [0064] does not

result in a grant to the server and services of the sever such as recited in claim 1. Furthermore, in Briscoe et al. the first signature is a so-called "time confidential information," which is a hash of the local server secret information and the current time parameter t (paragraph [0063]), and the second signature is a signature using the client's verification information and its authentication information (paragraph [0064]). These two signatures do not correspond to the hash value as recited in claim 1 of the present invention.

Further, we agree with the Examiner that Briscoe et al. does not teach using a protocol to prevent a man-in-the-middle attack.

In view of the above, the present invention as recited in amended claim 1 differs significantly from the disclosure of Briscoe et al. For instance, claim 1 is novel in view of the disclosure of Briscoe et al. in that a hash value of parameters including a nonce value transmitted from the server is received from the client computer. Briscoe et al. does not teach or suggest would not teach a person of ordinary skill in the art the features recited in claim 1.

Further, in view of the number of the above-mentioned differences between the present invention as recited in claim 1 and the disclosure of Briscoe et al., a person skilled in the art turning to the document of Alkhatib et al. would not find the necessary information to implement the authentication protocol as defined by the present invention as recited in claim 1.

In particular, Alkhatib et al. does not disclose an authentication procedure in which a hash value of parameters including a nonce value transmitted from the server is received from the client computer. Instead, Alkhatib et al. discloses that a member agent sends an initial request packet to a VCN manager (paragraph [0148]), the packet comprising a number of parameters among which a member seed which is a random number to thwart so called "man-in-the-middle" attacks (paragraph [0151]). The VCN manager then sends an acknowledgement packet (paragraph [0155]), the acknowledgement packet comprising the member seed sent by the member agent (paragraph [0157]). Thus, in contrast to the present invention as recited in claim 1, the member seed is sent from the member to the manager and there is no hash algorithm used in the authentication procedure of Alkhatib et al.

Further, it is noted that Alkhatib does not disclose upon which criteria the VCN manager acknowledges authentication (see [0154]-[0155]). Thus, in contrast to the present invention, Alkhatib does not disclose an authentication procedure utilizing a challenge

response pattern, at least not the challenge response pattern disclosed in claim 1 where a hash value is computed by the server and compared by the server with a hash value computed and sent by the client. It is noted that Briscoe et al. does not either disclose the comparison of two hash values during the authentication procedure.

Consequently, the present invention as defined by the present claims is not obvious in view of the disclosure of the cited prior art documents including Briscoe et al. and Alkhatib et al.

As mentioned above and in our Response filed on November 29, 2007, Briscoe et al. teaches an authentication method that consists of two steps while the authentication procedure of the present invention as recited at least in claim 1 is a simple one step process. The present invention as recited in the claims also differs in that the authentication method does not rely upon the existence of other clients within the network. In the authentication method of Briscoe et al., a client is required to gather authentication information from three other clients. Moreover, in the document of Briscoe et al., a hash algorithm is used during the distribution procedure for verification of messages and not for authentication. Alkhatib et al. also does not disclose the use of a hash algorithm for authentication.

The parameters used in the authentication procedure of the present invention differ from the parameters used in the authentication procedure disclosed by Alkhatib et al. and in the authentication procedure disclosed by Briscoe et al.

Applicant submits that the remaining independent claims and dependent claims related thereto are also allowable over the cited prior art at least for the reasons described above.

In light of the above remarks, Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: June 9, 2008

Peter G. Thurlow 47,138

Peter G. Thurlow (Reg. No.)
JONES DAY
222 East 41st Street
New York, New York 10017-6702
(212) 326-3694